Method and Apparatus for Creating a Message Digest Using a One-Way Hash Algorithm

Abstract of the Disclosure

A one-way hash algorithm is implemented in hardware and/or software. The hash algorithm creates a message digest from an input message. During one 16-operation round of the hash algorithm, a front computation process (202, Figure 2) computes a portion of a first operation. Then a systolic computation process (204, Figure 2) computes the remainder of the first operation and the next fifteen operations to complete the round. The systolic computation process pre-calculates (325, Figure 3) a portion of the next round in parallel with the completion of the current round. Because the systolic computation process has a shallower logic depth, and because certain calculations are done in parallel, an approximately four times reduction in the time to compute one round can be achieved. In one embodiment, the message digest computed by the hash algorithm is identical to a message digest computed using a conventional MD5 implementation, when given the same input message.